THOMSON DERWENT

MACHINE-ASSISTED TRANSLATION (MAT):

(19)【発行国】 日本国特許庁（ＪＰ）	**(19)[ISSUING COUNTRY]** Japan Patent Office (JP)
(12)【公報種別】 公開特許公報（Ａ）	**(12)[GAZETTE CATEGORY]** Laid-open Kokai Patent (A)
(11)【公開番号】 特開平 11-98134	**(11)[KOKAI NUMBER]** Unexamined Japanese Patent Heisei 11-98134
(43)【公開日】 平成１１年（１９９９）４月９日	**(43)[DATE OF FIRST PUBLICATION]** April 9, Heisei 11 (1999. 4.9)
(54)【発明の名称】 クッキーの改ざん・コピー検出処理方法およびプログラム記憶媒体	**(54)[TITLE OF THE INVENTION]** Alteration * copy detection processing method and program store medium of cookies
(51)【国際特許分類第６版】 H04L 9/32 G06F 13/00 357 G09C 1/00 610 640	**(51)[IPC INT. CL. 6]** H04L 9/32 G06F 13/00 357 G09C 1/00 610 640
【ＦＩ】 H04L 9/00 675 B G06F 13/00 357 Z G09C 1/00 610 C 640 B	**[FI]** H04L 9/00 675 B G06F 13/00 357 Z G09C 1/00 610 C 640 B
【審査請求】 未請求	**[REQUEST FOR EXAMINATION]** No

【請求項の数】 4 [NUMBER OF CLAIMS] 4

【出願形態】 ＯＬ [FORM of APPLICATION] Electronic

【全頁数】 8 [NUMBER OF PAGES] 8

(21)【出願番号】
特願平 9-258424

(21)[APPLICATION NUMBER]
Japanese Patent Application Heisei 9-258424

(22)【出願日】
平成９年（１９９７）９月２４日

(22)[DATE OF FILING]
September 24, Heisei 9 (1997. 9.24)

(71)【出願人】

【識別番号】
000004226

【氏名又は名称】
日本電信電話株式会社

【住所又は居所】

(71)[PATENTEE/ASSIGNEE]

[ID CODE]
000004226

[NAME OR APPELLATION]
Nippon Telegraph and Telephone CORP.

[ADDRESS OR DOMICILE]

(71)【出願人】

【識別番号】
000102739

【氏名又は名称】
エヌ・ティ・ティ・アドバンステクノロジ株式会社

【住所又は居所】

(71)[PATENTEE/ASSIGNEE]

[ID CODE]
000102739

[NAME OR APPELLATION]
NTT advance technology incorporated company

[ADDRESS OR DOMICILE]

(72)【発明者】

【氏名】
菊池　満孝

【住所又は居所】

(72)【発明者】

【氏名】
浅沼　透

【住所又は居所】

(74)【代理人】

【弁理士】

【氏名又は名称】
小笠原　吉義　（外１名）

(57)【要約】

【課題】
ＷＷＷサービス提供側でのＣｏｏｋｉｅの改ざん検出，Ｃｏｏｋｉｅのコピー使用の検出を可能とし，Ｃｏｏｋｉｅの不正利用を防止してＷＷＷサービスのセキュリティを維持する。

【解決手段】
ＷＷＷサービスを提供する計

(72)[INVENTOR]

[NAME OR APPELLATION]
Kikuchi　Mitsutaka

[ADDRESS OR DOMICILE]

(72)[INVENTOR]

[NAME OR APPELLATION]
Asanuma　Toru

[ADDRESS OR DOMICILE]

(74)[AGENT]

[PATENT ATTORNEY]

[NAME OR APPELLATION]
Ogasawara　Yoshigi　(et al.)

(57)[ABSTRACT OF THE DISCLOSURE]

[SUBJECT OF THE INVENTION]
Alteration detection of Cookie by the side of WWW service provision and detection of copy use of Cookie are enabled, illegal use of Cookie is prevented, and security of WWW service is maintained.

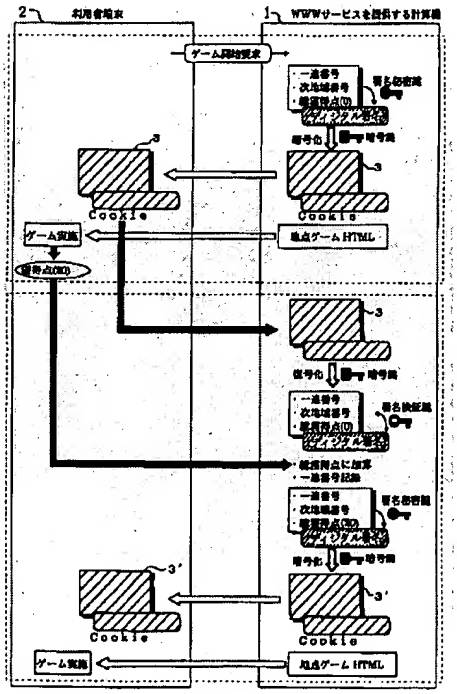
[PROBLEM TO BE SOLVED]
If there is service request from user terminal 2,

算機１は，利用者端末２からサービス要求があると，Ｃｏｏｋｉｅに一連または特定の情報を付加し，それにディジタル署名を付加して暗号化することにより，Ｃｏｏｋｉｅのデータ構造を隠蔽して送付する。利用者端末２からＣｏｏｋｉｅを受信すると，それを復号し，ディジタル署名を抽出して検証する。また，提供しているＷＷＷサービス項目と利用者との関係の一意性を，Ｃｏｏｋｉｅに付加した一連または特定の情報によって確認する。

by adding a series of or specific information to Cookie, adding digital signature to it, and enciphering, computer 1 which provides WWW service will conceal data structure of Cookie, and will be sent.

If Cookie is received from user terminal 2, it will be decoded, and digital signature will be extracted and verified.

Moreover, the uniqueness of relationship of WWW service item and user who provide is checked using a series of or specific information added to Cookie.



1-Computer which provides WWW service

2- User terminal

-- start request for games-->

Consecutive number
The following area number
The total acquiring point
--> signature secret key
Digital signature
Encryption | Code following

game implementation <-- point game HTML
|
Acquiring point (20)

3-
Encryption | Encryption key
Series code
The following area number
Acquiring point (D)
<--> signature verification key
Digital signature
Encryption | Encryption key
game implementation <-- point game HTML

【特許請求の範囲】

【請求項１】
WWWサービスを提供する計算機で，クッキーを用いて利用者に提供するサービスの遷移の制御，サービス間でのデータの継承を行う方法において，クッキーに一連または特定の情報を付加する過程と，少なくとも前記一連または特定の情報を付加したクッキーのデータを暗号化して送付する過程と，前記暗号化したクッキーを受信したときにクッキーを復号する過程と，

[CLAIMS]

[CLAIM 1]
Alteration * copy detection processing method of cookie wherein, in method of performing succession of data during transient control and transient service of service with which user is provided by computer which provides WWW service using cookie, it has
process which adds a series of or specific information to cookie, process in which data of cookie which added at least the above-mentioned a series of or specific information are enciphered and sent, process which decodes cookie when said enciphered

提供しているWWWサービス項目と利用者との関係の一意性を，前記クッキーに付加した一連または特定の情報によって確認する過程とを有し，WWWサービスのセキュリティを維持することを特徴とするクッキーの改ざん・コピー検出処理方法。

cookie is received, and process in which the uniqueness of relationship of WWW service item and user who provide is checked using a series of or specific information added to said cookie,
and security of WWW service is maintained.

【請求項２】

WWWサービスを提供する計算機で，クッキーを用いて利用者に提供するサービスの遷移の制御，サービス間でのデータの継承を行う方法において，クッキーに一連または特定の情報を付加する過程と，前記一連または特定の情報を付加したクッキーにディジタル署名を付加する過程と，前記ディジタル署名を付加したクッキーのデータを暗号化する過程と，暗号化したクッキーを送付する過程と，前記暗号化したクッキーを受信したときにクッキーを復号する過程と，復号したデータからディジタル署名を抽出し，ディジタル署名を検証する過程と，提供しているWWWサービス項目と利用者との関係の一意性を，前記クッキーに付加した一連または特定の情報によって確認する過程とを有し，WWWサービスのセキュリティを維持することを特徴とするクッキーの改ざん・コピー検出処理方法。

[CLAIM 2]

Alteration * copy detection processing method of cookie wherein, in method of performing succession of data between transient control of service with which user is provided by computer which provides WWW service using cookie, and service, it has
process which adds a series of or specific information to cookie; and process which adds digital signature to cookie which added said a series of or specific information, process which enciphers data of cookie which added said digital signature, process in which enciphered cookie is sent, and process which decodes cookie when said enciphered cookie is received, process in which extract digital signature from decoded data and digital signature is verified, and process in which the uniqueness of relationship of WWW service item and user who provide is checked using a series of or specific information added to said cookie, and security of WWW service is maintained.

【請求項３】
WWWサービスを提供する計算機で実行される，クッキーの改ざんまたはコピーによる不正利用を検出するためのプログラムを記憶したプログラム記憶媒体であって，クッキーに一連または特定の情報を付加する処理と，少なくとも前記一連または特定の情報を付加したクッキーのデータを暗号化して送付する処理と，前記暗号化したクッキーを受信したときにクッキーを復号する処理と，提供しているWWWサービス項目と利用者との関係の一意性を，前記クッキーに付加した一連または特定の情報によって確認する処理とを計算機に実行させるプログラムを格納したことを特徴とするプログラム記憶媒体。

[CLAIM 3]
Program store medium that stores program which makes computer perform processing which is program store medium on which was stored program for detecting illegal use by alteration or copy of cookie performed by computer which provides WWW service, and adds a series of or specific information to cookie, processing which enciphers and sends data of cookie which added at least the above-mentioned a series of or specific information, processing which decodes cookie when said enciphered cookie is received, and processing which checks the uniqueness of relationship of WWW service item and user who provide using a series of or specific information added to said cookie.

【請求項４】
WWWサービスを提供する計算機で実行される，クッキーの改ざんまたはコピーによる不正利用を検出するためのプログラムを記憶したプログラム記憶媒体であって，クッキーに一連または特定の情報を付加する処理と，前記一連または特定の情報を付加したクッキーにディジタル署名を付加する処理と，前記ディジタル署名を付加したクッキーのデータを暗号化する処理

[CLAIM 4]
Program store medium on which is stored program for detecting illegal use by alteration or copy of cookie performed by computer which provides WWW service,
processing which adds digital signature to cookie which added said a series of or specific information, processing which enciphers data of cookie which added said digital signature, processing which sends enciphered cookie, and processing which decodes cookie when said enciphered cookie is received, processing which extracts digital signature from decoded

と，暗号化したクッキーを送付する処理と，前記暗号化したクッキーを受信したときにクッキーを復号する処理と，復号したデータからディジタル署名を抽出し，ディジタル署名を検証する処理と，提供しているWWWサービス項目と利用者との関係の一意性を，前記クッキーに付加した一連または特定の情報によって確認する処理とを計算機に実行させるプログラムを格納したことを特徴とするプログラム記憶媒体。

data and verifies digital signature, and program which makes computer perform processing which checks the uniqueness of relationship of WWW service item and user who provide using a series of or specific information added to said cookie.

【発明の詳細な説明】

[DETAILED DESCRIPTION OF THE INVENTION]

【０００１】

[0001]

【発明の属する技術分野】

本発明は，クッキー（Ｃｏｏｋｉｅ）の改ざんおよびコピーを，ディジタル署名技術，暗号化技術，Ｃｏｏｋｉｅへの一連または特定の情報（番号）の付与により検出する方法およびそれを実現するためのプログラムを格納したプログラム記憶媒体に関する。

[TECHNICAL FIELD OF THE INVENTION]

This invention relates to program store medium on which was stored program for implementing method of detecting alteration and copy of cookie (Cookie) by providing of digital signature technique, encoding technology, and a series of or specific information (number) on Cookie.

【０００２】

[0002]

【従来の技術】

Ｃｏｏｋｉｅは，WWW (World

[PRIOR ART]

Cookie is information used in order that WWW

Wide Web）サービスを提供する計算機であるＷＷＷサーバが，利用者に提供するサービスの遷移の制御，サービス間でのデータの継承を行うために用いる情報であり，ＷＷＷブラウザがＷＷＷサーバにアクセスした際にＷＷＷサーバからＷＷＷブラウザへ送付され，その後，ＷＷＷブラウザがＷＷＷサーバにアクセスするときに，ＨＴＴＰヘッダに埋め込まれてＷＷＷサーバに転送されるようになっているものである。

server which is computer which provides WWW (World Wide Web) service may perform succession of data between transient control of service with which user is provided, and service, when WWW browser accessed WWW server, it is sent to WWW browser from WWW server and WWW browser accesses WWW server after that, is embedded at HTTP header and transmitted to WWW server.

【０００３】

従来，ＷＷＷサーバからＷＷＷブラウザへ送付されたＣｏｏｋｉｅは，利用者端末において，ＷＷＷブラウザの定める特定のファイルに記述され，端末利用者によって書き換えやコピーが可能であるため，ＷＷＷサーバは，受信したＣｏｏｋｉｅが書き換えやコピーされたものであっても，それを検出することができなかった。

[0003]

Since Cookie sent to WWW browser from WWW server was formerly described in user terminal by specific file which WWW browser defines and overwrite and copy were made by terminal user, WWW server was not able to detect it, even if it rewrote and copied Cookie which received.

【０００４】

[0004]

【発明が解決しようとする課題】

Ｃｏｏｋｉｅを用いて利用者のサービスの遷移を制御するＷＷＷサービスの提供において，従来の方法では，利用者がＣｏｏ

[PROBLEM TO BE SOLVED BY THE INVENTION]

In provision of WWW service which controls transition of service of user using Cookie, by conventional method, when user overwrites Cookie, WWW service is controlled unjustly, or

ｋｉｅを書き換えることにより不正にWWWサービスを制御したり，利用者がＣｏｏｋｉｅをコピーし，第三者に渡すかまたは第三者がネットワーク上でＣｏｏｋｉｅをモニタすることにより入手したりして，不正にWWWサービスを利用することができるという問題がある。

when user copies Cookie, and hands third person or third person does monitor of the Cookie on network, it acquires, and there is problem that WWW service can be utilized irregularly.

【０００５】

本発明は，上記の問題点に鑑みてなされたもので，その目的とするところは，WWWサービス提供側でのＣｏｏｋｉｅの改ざん検出，Ｃｏｏｋｉｅのコピー使用の検出を可能とし，Ｃｏｏｋｉｅの不正利用を防止してWWWサービスのセキュリティを維持する手段を提供することにある。

[0005]

It is providing means this invention's being made in view of the above-mentioned problem, and place made into the objective enabling alteration detection of Cookie by the side of WWW service provision, and detection of copy use of Cookie, preventing illegal use of Cookie, and maintaining security of WWW service.

【０００６】

[0006]

【課題を解決するための手段】

上記目的を達成するため，本発明は，Ｃｏｏｋｉｅにディジタル署名を付加することによるWWWサービス提供側でのＣｏｏｋｉｅの改ざん検出，Ｃｏｏｋｉｅへの一連番号付与によるＣｏｏｋｉｅのコピー使用の検出を可能とするもので，Ｃｏｏｋｉｅの暗号化と併せ，高いセキュリティを達成し得るようにするものである。具体的には，例

[MEANS TO SOLVE THE PROBLEM]

Since the above-mentioned objective is attained, this invention enables alteration detection of Cookie by the side of WWW service provision by adding digital signature to Cookie, and detection of copy use of Cookie by consecutive-number providing to Cookie, combines with encryption of Cookie, and enables it to attain high security.

Specifically, for example, as follows, it processes.

えば次のように処理する。

【０００７】
WWWサービスを提供する計算機は，ディジタル署名を作成するための署名秘密鍵とディジタル署名を検証するための署名検証鍵および暗号化のための秘密鍵を持ち，利用者端末から初期のサービス利用要求があったとき，利用者の次のサービス要求を決定する情報および唯一の一連番号，さらに利用者から入手したデータがあるときにはそのデータまたはその初期データを含むデータの集合に対し署名秘密鍵でディジタル署名を作成し，上記データの集合と共に暗号化の秘密鍵で暗号化し，Ｃｏｏｋｉｅとして利用者端末に送付する。

[0007]
Computer which provides WWW service is information and the only consecutive number which opt for the next service request of user when it has secret key for signature verification key for verifying signature secret key for making digital signature, and digital signature, and encryption and there is service utilization request of initial stage from user terminal, when there are data which acquired from user more, digital signature is made with signature secret key to data aggregate containing the data or its initial-stage data, and it enciphers with secret key of encryption with the above-mentioned data aggregate, and sends to user terminal as Cookie.

【０００８】
また，WWWサービスを提供する計算機は，利用者端末からサービス遷移要求があったとき，暗号化の秘密鍵を用いて受信したＣｏｏｋｉｅを復号し，署名検証鍵を用いてディジタル署名を検証し，署名検証に失敗した場合には，利用者または第三者によるＣｏｏｋｉｅの改ざんが行われたとみなしてサービスを直ちに停止する。署名検出に成功した場合には，正常なサービス遷移要求とみなし，利用者の

[0008]
Moreover, when there is service transient request from user terminal, Cookie which received using secret key of encryption is decoded, digital signature is verified using signature verification key and signature verification goes wrong, computer which provides WWW service considers that alteration of Cookie by user or third person is performed, and stops service immediately.
When successful in signature detection, it is regarded as normal service transient request, digital signature is made with signature secret key to data aggregate which acquired from data

次のサービス要求を制御するデータ，受信したＣｏｏｋｉｅと同一の一連番号および利用者から入手したデータの集合に対し署名秘密鍵でディジタル署名を作成し，上記データの集合と共に暗号化の秘密鍵で暗号化し，Ｃｏｏｋｉｅとして利用者端末に送付する。

which control the next service request of user, consecutive number of the same as Cookie which received, and user, and it enciphers with secret key of encryption with the above-mentioned data aggregate, and sends to user terminal as Cookie.

【０００９】
また，WWWサービスを提供する計算機は，利用者端末からサービス遷移要求があったとき，受信したＣｏｏｋｉｅから入手した一連番号をサービス識別情報と共に記録し，これ以後，一つのサービス識別情報に対し２回以上同一の一連番号が記録されていれば，その一連のサービス遷移において第三者がＣｏｏｋｉｅをコピーし不正利用が行われたとみなす。

[0009]
Moreover, computer which provides WWW service records consecutive number which acquired from Cookie which received when there was service transient request from user terminal with service discriminative information, and after this, if the consecutive number same twice or more is recorded to one service discriminative information, in the service transition of a series of, third person will copy Cookie and will consider that illegal use is performed.

【００１０】
特に，ディジタル署名の作成および検証には，例えばＥＳＩＧＮ（Efficientdigital SIGNature scheme）を用いると，高度なセキュリティを高速に実現することができる。また，暗号化および復号化には，例えば手順公開型の高速暗号化アルゴリズムであるＦＥＡＬ（Fast data Encipherment ALgorithm）を用いると，高速処理が可能である

[0010]
In particular, if ESIGN (Efficientdigital SIGNature scheme) is used, high degree security is realizable for creation and verification of digital signature at high speed.
Moreover, when FEAL (Fast data Encipherment ALgorithm) which is procedure public presentation, for example, type high-speed encryption algorithm is used for encryption and decoding, since high-speed processing can be performed, it is desirable.

ため望ましい。

【００１１】
以上の処理方法をコンピュータによって実現するためのプログラムは，コンピュータが読み取り可能な可搬媒体メモリ，半導体メモリ，ハードディスクなどの適当な記憶媒体に格納することができる。

[0011]
Program for computer to implement the above processing method is storable in suitable storage storagemedia, such as portable medium memory which can read and do computer, semiconductor memory, and hard disk.

【００１２】

[0012]

【発明の実施の形態】
以下，図面を用いて本発明の具体的な実施の形態について説明する。図１は本発明を実施するシステムの構成例を示す。

[EMBODIMENT OF THE INVENTION]
Hereafter, concrete Embodiment of this invention is illustrated using drawing.
FIG. 1 shows example of composition of system which implements this invention.

【００１３】
図中，１はWWWサービスを提供する計算機（WWWサーバ），１１はWWWサービスのサービスプログラム，１２は利用者のサービス要求に対してＣｏｏｋｉｅに付与する一連番号を管理する一連番号管理部，１３はＣｏｏｋｉｅを生成するＣｏｏｋｉｅ生成部，１４はＣｏｏｋｉｅの改ざん・コピーが行われていないかどうかを検証するＣｏｏｋｉｅ検証部，１５はＣｏｏｋｉｅに付与するディジタル署名を作成および検証する署名作成・検証部，１６はＣｏｏｋｉｅの暗号化および復号化を行う

[0013]
In the drawing(s), computer (WWW server) by which 1 provides WWW service, and 11 are service programs of WWW service, 12 is a consecutive-number management part which manages consecutive number which provides to Cookie to service request of user, 13 is a Cookie generation part which forms Cookie, 14 is a Cookie verification part which verifies whether alteration * copy of Cookie is performed, 15 is a signature creation * verification part which makes and verifies digital signature which provides to Cookie, 16 is an encryption * decoding part which performs encryption and decoding of Cookie, 17 is a HTTP daemon who controls transmitting and receiving of data based on HTTP (Hypertext

暗号化・復号化部，１７はＨＴＴＰ（Hypertext TransferProtocol)によるデータの送受信を制御するＨＴＴＰデーモン，１８はＣｏｏｋｉｅに付与する一連番号の最大値を記憶しておくための一連番号最大値管理ファイルを表す。

TransferProtocol), 18 expresses consecutive-number maximum-value management file for storing maximum value of consecutive number which provides to Cookie.

【００１４】

署名作成・検証部１５が使用するディジタル署名作成用の署名秘密鍵とディジタル署名検証用の署名検証鍵，および暗号化・復号化部１６が使用する暗号化用の暗号鍵は，計算機１のディスクまたはメモリ上に保持されている。

[0014]

Signature secret key for digital signature creation and signature verification key for digital signature verification which signature creation * verification part 15 uses, and encryption key for encryption which encryption * decoding part 16 uses is maintained on disc of computer 1, or memory.

【００１５】

また，２はWWWサービスを利用する利用者端末，２１はWWWサービスによって提供される情報の表示および入力を行うためのブラウザ，２２はＣｏｏｋｉｅを所定のファイル等に書き込むＣｏｏｋｉｅ書込み部，２３はWWWサービスを提供する計算機１にＣｏｏｋｉｅを通知するためにＣｏｏｋｉｅを読み込むＣｏｏｋｉｅ読込み部，２４はＣｏｏｋｉｅを保存する所定のファイル等のＣｏｏｋｉｅ格納部を表す。

[0015]

Moreover, 2 is user terminal using WWW service, 21 is browser for performing display and input of information which are provided by WWW service, 22 is a Cookie write-in part which writes Cookie in fixed file etc., 23 is a Cookie reading part which reads Cookie in order to notify Cookie to computer 1 which provides WWW service, 24 expresses Cookie storing parts, such as fixed file which saves Cookie.

【００１６】

[0016]

Ｃｏｏｋｉｅ書込み部２２およびＣｏｏｋｉｅ読込み部２３は，ブラウザ２１に内蔵されている機能であり，ブラウザ２１が，例えば米国Ｎｅｔｓｃａｐｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ社が開発したＮｅｔｓｃａｐｅ Ｎａｖｉｇａｔｏｒである場合，Ｃｏｏｋｉｅが格納されるＣｏｏｋｉｅ格納部２４は「 ～Netscape¥Navigator¥Cookies.txt」のファイルである。また，ブラウザ２１が，米国Ｍｉｃｒｏｓｏｆｔ社が開発したＩｎｔｅｒｎｅｔ Ｅｘｐｌｏｒｅｒの場合，Ｃｏｏｋｉｅ格納部２４ は「¥Windows¥Cookies¥XXX.txt」のファイルである。

Cookie write-in part 22 and Cookie reading part 23 are functions built in browser 21, and browser 21 of Cookie storing part 24 in which Cookie is stored is file of "-Netscape¥Navigator¥Cookies.txt" when it is Netscape Navigator which USA NetscapeCommunications developed.
Moreover, when browser 21 is Internet Explorer which USA Microsoft developed, Cookie storing part 24 is file of "¥Windows¥Cookies¥XXX.txt."

【００１７】
図２は，本発明の一実施形態の作用を説明するための図である。本実施の形態では，ＷＷＷサービスを提供する計算機１は，いくつかの擬似的な地点を遷移しながらゲームが展開する形態の地点毎のゲームを，利用者端末２に提供するものとする。

[0017]
FIG. 2 is figure for illustrating effect of one embodiment of this invention.
In this Embodiment, computer 1 which provides WWW service shall provide user terminal 2 with game for every point of form which game expands, while shifting some pseudo points.

【００１８】
利用者端末２からゲームの開始を要求すると，計算機１では，サービスプログラム１１の制御

[0018]
If start of game is required from user terminal 2, by computer 1
On basis of control of service program 11,

のもとに，一連番号管理部１２により一連番号最大値管理ファイル１８を読み込んで，新規にこの要求のみに唯一な一連番号を付与し，次に行うゲームの地点識別子（次地域番号）を決定し，総獲得点を初期設定する。次に，Ｃｏｏｋｉｅの生成にあたって，Ｃｏｏｋｉｅ生成部１３は署名作成・検証部１５を呼び出し，一連番号，次地域番号，総獲得点の３つのデータ集合に対し，ＥＳＩＧＮの署名秘密鍵によりディジタル署名を作成し，さらに暗号化・復号化部１６を呼び出して，ＦＥＡＬ暗号鍵によりそれらを暗号化し，Ｃｏｏｋｉｅを生成する。

consecutive-number maximum-value management file 18 is read by consecutive-number management part 12, consecutive number only is anew provided only to this request, next, point identifier (the following area number) of game to perform is decided, and initialization of the total acquiring point is carried out.

Next, in generation of Cookie, Cookie generation part 13 calls signature creation * verification part 15, to three data ensembles, consecutive number, the following area number, and the total acquiring point, makes digital signature with signature secret key of ESIGN, furthermore, calls encryption * decoding part 16, enciphers them with FEAL encryption key, and forms Cookie.

【００１９】

なお，このＣｏｏｋｉｅのディジタル署名の作成および検証に用いるＥＳＩＧＮ（Efficient digital SIGNature scheme）については，参考文献として，例えば特開昭６２－１１３１９１号公報，特開平０１－１４７５８５号公報，特開平０３－１２９３８４号公報がある。また，Ｃｏｏｋｉｅの暗号化および復号化に用いるＦＥＡＬ（Fast data Encipherment ALgorithm）については，参考文献として，特開昭６０－１９６０５９号公報，特開昭６１－２００７７８号公報がある。

[0019]

Furthermore, about ESIGN (Efficient digital SIGNature scheme) used for creation and verification of digital signature of this Cookie, there are Unexamined-Japanese-Patent No. 62-113191, Unexamined-Japanese-Patent No. 01-147585,03-129384 as bibliography.

Moreover, about FEAL (Fast data Encipherment ALgorithm) used for encryption and decoding of Cookie, there are Unexamined-Japanese-Patent No. 60-196059,61-200778 as bibliography.

【００２０】
以上のようにしてディジタル署名を付与して暗号化したＣｏｏｋｉｅ３を，当該地点のゲームを実行するＨＴＭＬファイルと共に，ＨＴＴＰデーモン１７を介して利用者端末２に送付する。

[0020]
Cookie3 which digital signature was provided as mentioned above and enciphered is sent to user terminal 2 through HTTP daemon 17 with HTML file which performs game of said point.

【００２１】
利用者端末２では，ブラウザ２１によりＨＴＭＬファイルとＣｏｏｋｉｅ３を受信すると，Ｃｏｏｋｉｅ書込み部２２より，Ｃｏｏｋｉｅ格納部２４にＣｏｏｋｉｅ３を保存する。

[0021]
At user terminal 2, if browser 21 receives HTML file and Cookie3, Cookie3 is saved in Cookie storing part 24 from Cookie write-in part 22.

【００２２】
次に，利用者端末２で利用者がゲームを実行し，次の地点のゲームを実行するため再び計算機１に要求を発行する際，Ｃｏｏｋｉｅ読込み部２３によりＣｏｏｋｉｅ格納部２４からＣｏｏｋｉｅ３を読み出し，今回取得したゲームの獲得点とＣｏｏｋｉｅ３を計算機１へ送付する。

[0022]
Next, in order for user to perform game at user terminal 2 and to perform game of the next point, when publishing request to computer 1 again, Cookie3 is read from Cookie storing part 24 by Cookie reading part 23, and acquiring point of game acquired this time and Cookie3 are sent to computer 1.

【００２３】
計算機１では，ＨＴＴＰデーモン１７を介して利用者端末２からのゲームの継続要求を受けると，サービスプログラム１１は，Ｃｏｏｋｉｅ検証部１４を呼び出す。Ｃｏｏｋｉｅ検証部１４

[0023]
By computer 1, if continuation request of game from user terminal 2 is received through HTTP daemon 17, service program 11 will call Cookie verification part 14.
Cookie verification part 14 calls encryption * decoding part 16 first, and decodes Cookie with

は，まず暗号化・復号化部１６を呼び出してＦＥＡＬ暗号鍵によりＣｏｏｋｉｅを復号する。その後，Ｃｏｏｋｉｅ検証部１４は，署名作成・検証部１５を呼び出し，ＥＳＩＧＮ署名検証鍵によりディジタル署名を検証する。

FEAL encryption key.
After that, Cookie verification part 14 calls signature creation * verification part 15, and verifies digital signature with ESIGN signature verification key.

【００２４】
サービスプログラム１１は，ディジタル署名の検証に失敗したときには，Ｃｏｏｋｉｅが改ざんされたとみなして直ちにサービス続行を取り消す。検証に成功したときには，利用者端末２から送付された獲得点を総獲得点に加算し，次に行うゲームの地点識別子を決定し，受信したＣｏｏｋｉｅ３から一連番号を抽出し，それらの３つのデータ集合に対し，署名作成・検証部１５によってＥＳＩＧＮの署名秘密鍵によりディジタル署名を作成し，暗号化・復号化部１６によりＦＥＡＬ暗号鍵を用いて暗号化し，Ｃｏｏｋｉｅ３′を作成し，当該地点のゲームを実行するＨＴＭＬファイルと共に利用者端末２に送付する。

[0024]
When verification of digital signature goes wrong, service program 11 considers that Cookie is altered and cancels service continuation immediately.
When successful in verification, acquiring point sent from user terminal 2 is added to the total acquiring point, next, point identifier of game to perform is decided and consecutive number is extracted from Cookie3 which received, digital signature is made with signature secret key of ESIGN by signature creation * verification part 15 to those three data ensembles, it enciphers using FEAL encryption key by encryption * decoding part 16, Cookie3' is made, and it sends to user terminal 2 with HTML file which performs game of said point.

【００２５】
上記の処理で受信したＣｏｏｋｉｅ３から抽出した一連番号は，ゲームの識別子と共に計算機１のディスクに記録し，以後，

[0025]
When consecutive number extracted from Cookie3 which received by the above-mentioned processing is recorded on disc of computer 1 with identifier of game and

同一の一連番号とゲーム識別子の組が複数回記録されていた場合には，Ｃｏｏｋｉｅの不正なコピーがなされたとみなす。

several times of recording of the group of the same consecutive number and game identifier is carried out after that, it is considered that illegitimate copy of Cookie is made.

【００２６】

以上の実施の形態では，Ｃｏｏｋｉｅにより，利用者のゲーム実施地点の遷移と総獲得点の記録を計算機１の完全主導で制御することで正常な実施が成り立っており，利用者によるゲーム実施地点および総獲得点の改ざんを，ディジタル署名を付加することにより計算機１で検出可能としている。

[0026]

In the above Embodiment, cookie, normal implementation is formed by controlling transition of user's game implementation point, and recording of the total acquiring point by full initiative of computer 1, alteration of game implementation point by user and the total acquiring point is made detectable by computer 1 by adding digital signature.

【００２７】

なお，利用者端末２でゲームを実施した結果のゲームの獲得点は，Ｃｏｏｋｉｅ３とは別に計算機１へ送付する。利用者端末２では，Ｃｏｏｋｉｅ３を保存するのみで暗号化・復号化を含め，一切の加工は行わない。例えば，本実施の形態におけるゲームの場合，ＷＷＷサーバからダウンロードするゲームプログラム内で点数をスクランブルすることにより，利用者端末２におけるゲーム点数の改ざんを防止しているが，これはＣｏｏｋｉｅの改ざん防止とは独立しており，直接的に関係する事項ではない。

[0027]

Furthermore, acquiring point of game of result which implemented game at user terminal 2 is sent to computer 1 apart from Cookie3.

No process is performed at user terminal 2, including encryption * decoding only by saving Cookie3.

For example, although alteration of game mark in user terminal 2 is prevented by carrying out scramble of the mark within game program which downloads from WWW server in the case of game in this Embodiment, it is not matter to which alteration prevention of Cookie is independent and this is directly related.

【００２８】
図３は，図１に示すサービスプログラム１１の処理フローチャートである。ステップＳ１では，利用者端末２からの要求に対し，初期アクセスかどうかを判定し，新たにゲームを開始することを要求する最初のアクセスであれば，ステップＳ２へ進み，一連番号管理部１２を呼び出し，要求に対してユニークな一連番号を付与する。その後，ステップＳ６へ進む。

[0028]
FIG. 3 is processing flowchart of service program 11 shown in FIG. 1.
In step S1, it judges whether it is initial-stage access to request from user terminal 2, and if it is the first access which requires that game should newly be started, it will progress to step S2, consecutive-number management part 12 will be called, and unique consecutive number will be provided to request.
After that, it progresses to step S6.

【００２９】
初期アクセスでなければ，ステップＳ３へ進み，Ｃｏｏｋｉｅ検証部１４を呼び出して，Ｃｏｏｋｉｅが改ざんされたものでないかをチェックする。また，Ｃｏｏｋｉｅがコピーされたものでないかどうかも併せてチェックする。この不正コピーのチェックは，例えばＣｏｏｋｉｅから抽出した一連番号とゲーム識別子（次地域番号）の組をその都度記録しておき，同一の一連番号とゲーム識別子の組が既に記録されているかどうかを調べることにより行うことができる。

[0029]
If it is not initial-stage access, it will progress to step S3, Cookie verification part 14 will be called, and it will confirm whether to be that by which Cookie was altered.
Moreover, it confirms collectively whether be that which copied Cookie.
Check of this illegal copy records group of consecutive number extracted from Cookie, and game identifier (the following area number) each time, and can be performed by examining whether group of the same consecutive number and game identifier is already recorded.

【００３０】
ステップＳ４の判定により，Ｃｏｏｋｉｅが改ざんまたはコピーされたものである場合には，

[0030]
When evaluation of step S4 alters or copies Cookie, it progresses to step S5 and service is stopped.

ステップＳ５へ進み，サービスを中止する。検証がＯＫであれば，ステップＳ６によりＣｏｏｋｉｅ生成部１３を呼び出してＣｏｏｋｉｅを生成する。続いてステップＳ７によりサービスのためのＨＴＭＬファイルを編集し，ＣｏｏｋｉｅとＨＴＭＬファイルを要求元の利用者端末２へ送付する。

If verification is O.K., Cookie generation part 13 will be called by step S6, and Cookie will be formed.
Then, HTML file for service is edited by step S7, and Cookie and HTML file are sent to user terminal 2 of requester.

【００３１】
図４は，図１に示す一連番号管理部１２の処理フローチャートである。一連番号管理部１２は，サービスプログラム１１から呼び出されると，まずステップＳ１１により，一連番号最大値管理ファイル１８に読み書きの競合防止のためのロックをかける。次に，ステップＳ１２では，一連番号最大値管理ファイル１８から現在記憶している一連番号の最大値を読み出す。ステップＳ１３では，読み出した一連番号に１をプラスし，ステップＳ１４により，その値を一連番号最大値管理ファイル１８に書き戻す。次に，ステップＳ１５では，一連番号最大値管理ファイル１８の読み書き競合防止のロックを解除し，サービスプログラム１１に一連番号を通知して処理を終了する。

[0031]
FIG. 4 is a processing flowchart of consecutive-number management part 12 shown in FIG. 1.
If call appearance of the consecutive-number management part 12 is carried out from service program 11, it will cover lock for competition prevention of read-write over consecutive-number maximum-value management file 18 by step S11 first.
Next, in step S12, maximum value of consecutive number stored now is read from consecutive-number maximum-value management file 18.
In step S13, 1 is added to read consecutive number and the value is returned to consecutive-number maximum-value management file 18 by step S14.
Next, in step S15, lock of read-write competition prevention of consecutive-number maximum-value management file 18 is released, consecutive number is notified to service program 11, and processing is completed.

【００３２】
図５（Ａ）は，図１に示すＣｏｏｋｉｅ生成部１３の処理フローチャートである。Ｃｏｏｋｉｅ生成部１３は，サービスプログラム１１からのＣｏｏｋｉｅ生成要求により，まずステップＳ２１においてＣｏｏｋｉｅ化対象データを１データ構造に編集する。次に，ステップＳ２２では，署名作成・検証部１５を呼び出し，Ｃｏｏｋｉｅ化対象データのデータ構造に対してディジタル署名を作成する。続いてステップＳ２３では，Ｃｏｏｋｉｅ化対象データのデータ構造とディジタル署名とを合成して，暗号化・復号化部１６により暗号化し，その結果を送付するＣｏｏｋｉｅとする。

[0032]
FIG.5(A) is a processing flowchart of Cookie generation part 13 shown in FIG. 1.
Cookie generation part 13 edits data for Cookie-izing into 1 data structure in step S21 by Cookie generation request from service program 11 first.
Next, in step S22, signature creation * verification part 15 is called, and digital signature is made to data structure of data for Cookie-izing.
Then, in step S23, data structure of data for Cookie-izing and digital signature are compounded, and it enciphers by encryption * decoding part 16, and is referred to as Cookie which sends the result.

【００３３】
図５（Ｂ）は，図１に示すＣｏｏｋｉｅ検証部１４の処理フローチャートである。Ｃｏｏｋｉｅ検証部１４は，サービスプログラム１１からのＣｏｏｋｉｅ検証要求により，まずステップＳ３１において利用者端末２から受け取ったＣｏｏｋｉｅを暗号化・復号化部１６によって復号する。ステップＳ３２では，復号した結果のＣｏｏｋｉｅ化対象データのデータ構造とディジタル署名を抽出し，ステップＳ３３により，ディジタル署名

[0033]
FIG.5(B) is a processing flowchart of Cookie verification part 14 shown in FIG. 1.
Cookie verification part 14 decodes Cookie first received from user terminal 2 in step S31 by Cookie verification request from service program 11 by encryption * decoding part 16.
In step S32, data structure of data for Cookie-izing of result and digital signature which were decoded are extracted, and it is verified by step S33 whether digital signature is rightful.
By step S34, verification result is judged, if verification result is O.K., return coding of Verification O.K. will be set up by step S35, and

が正当であるかどうかを検証する。ステップＳ３４により，検証結果を判定し，検証結果がＯＫであれば，ステップＳ３５により検証ＯＫのリターンコードを設定して，サービスプログラム１１に検証成功を報告する。検証結果がＮＧであれば，ステップＳ３６により検証ＮＧのリターンコードを設定し，サービスプログラム１１に検証失敗を報告する。

verification success will be reported to service program 11.
If verification result is NG, return coding of Verification NG will be set up by step S36, and verification failure will be reported to service program 11.

【００３４】
なお，サービスプログラム１１では，この復号したＣｏｏｋｉｅについてディジタル署名による検証のほか，要求ごとに一意に付与した一連番号により重複要求であるかどうかなどの検証を行う。

[0034]
Furthermore, in service program 11, consecutive number which provided uniquely for every request besides verification by digital signature about this decoded Cookie performs verification of whether to be duplication request.

【００３５】

【発明の効果】
以上説明したように，本発明によれば，利用者へのサービス提供の遷移をＣｏｏｋｉｅにより制御するＷＷＷサービスの提供において，利用者によるＣｏｏｋｉｅの改ざんおよびＣｏｏｋｉｅのコピーによるサービスの正常な実施への妨害を，Ｃｏｏｋｉｅにディジタル署名を付加することによりサービスを提供する計算機において検出するこ

[0035]

[ADVANTAGE OF THE INVENTION]
In provision of WWW service which, as explained above, controls transition of service provision to user by Cookie according to this invention, alteration of Cookie by user, and disturbance to normal implementation of service by copy of Cookie, by adding digital signature to Cookie, it can detect now in computer which provides service, and, furthermore, data structure of Cookie is concealed using encoding technology, by maintaining key used for digital signature and encryption only to computer

とが可能になり，さらに暗号技術を用いてＣｏｏｋｉｅのデータ構造を隠蔽し，ディジタル署名および暗号化に用いる鍵をサービスを提供する計算機にのみ保持することによって，高いセキュリティでWWWサービスを提供することができるようになる。

which provides service, WWW service can be provided now with high security.

【図面の簡単な説明】

[BRIEF DESCRIPTION OF THE DRAWINGS]

【図１】
本発明を実施するシステムの構成例を示す図である。

[FIG. 1]
It is figure showing example of composition of system which implements this invention.

【図２】
本発明の一実施形態の作用を説明するための図である。

[FIG. 2]
It is figure for illustrating effect of one embodiment of this invention.

【図３】
サービスプログラムの処理フローチャートである。

[FIG. 3]
It is processing flowchart of service program.

【図４】
一連番号管理部の処理フローチャートである。

[FIG. 4]
It is processing flowchart of consecutive-number management part.

【図５】
Ｃｏｏｋｉｅ生成部とＣｏｏｋｉｅ検証部の処理フローチャートである。

[FIG. 5]
It is processing flowchart of Cookie generation part and Cookie verification part.

【符号の説明】

[DESCRIPTION OF SYMBOLS]

1　WWWサービスを提供す

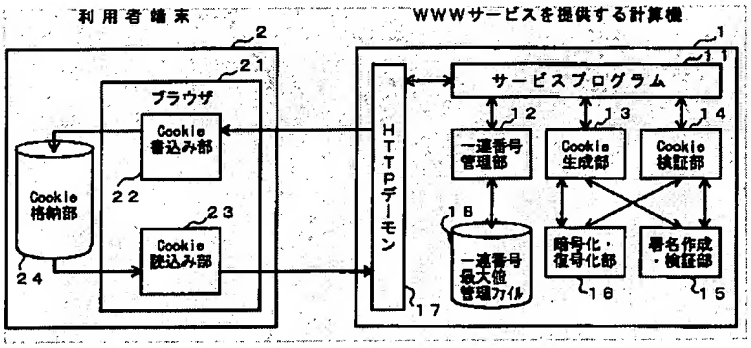
1　Computer which provides WWW service

る計算機
１１　サービスプログラム
１２　一連番号管理部
１３　Ｃｏｏｋｉｅ生成部
１４　Ｃｏｏｋｉｅ検証部
１５　署名作成・検証部
１６　暗号化・復号化部
１７　ＨＴＴＰデーモン
１８　一連番号最大値管理ファイル
２　利用者端末
２１　ブラウザ
２２　Ｃｏｏｋｉｅ書込み部
２３　Ｃｏｏｋｉｅ読込み部
２４　Ｃｏｏｋｉｅ格納部
３　Ｃｏｏｋｉｅ

11 Service program
12 Consecutive-number management part
13 Cookie generation part
14 Cookie verification part
15 Signature creation * verification part
16 Encryption * decoding part
17 HTTP daemon
18 Consecutive-number maximum-value management file
2 User terminal
21 Browser
22 Cookie write-in part
23 Cookie reading part
24 Cookie storing part
3 Cookie

【図１】

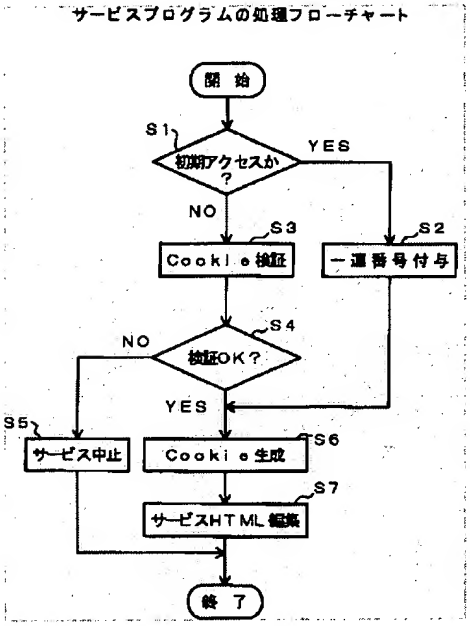
[FIG. 1]



1 Computer which provides WWW service
11 Service program
12 Consecutive-number management part
13 Cookie generation part
14 Cookie verification part
15 Signature creation * verification part
16 Encryption * decoding part
17 HTTP daemon
18 Consecutive-number maximum-value management file

2 User terminal
21 Browser
22 Cookie write-in part
23 Cookie reading part
24 Cookie storing part
3 Cookie

【図３】 [FIG. 3]

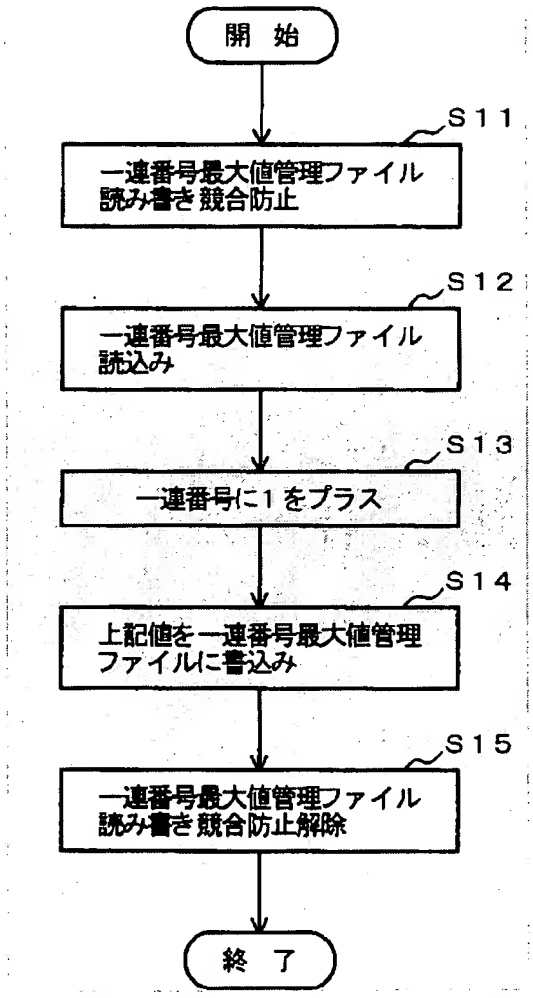


Processing flowchart of service program
Start
S1-initial-stage access?
S2 -number providing 1 consecutive number.
S3-Cookie verification
S4-verification O.K.
S5-service stop
S6-Cookie generation
S7-service HTML edit

Completion

【図４】 [FIG. 4]

一連番号管理部の処理フローチャート



Processing flowchart of consecutive-number management part

Start

S11- Consecutive-number maximum-value management file read-write

competition prevention

S12- Consecutive-number maximum-value management file reading

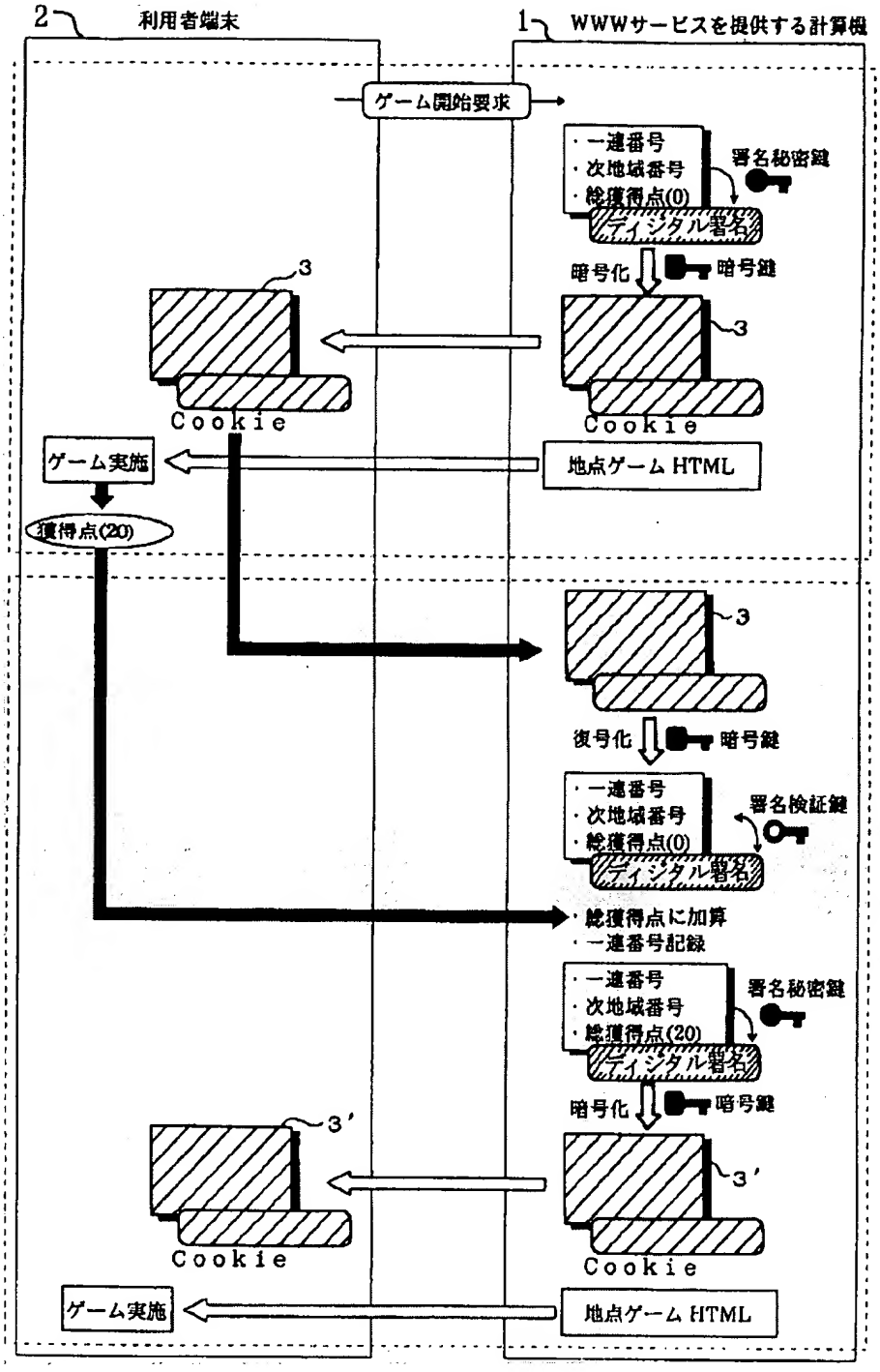
S13- 1 is added to consecutive number.

S14- The above-mentioned value is written in consecutive-number maximum-value management file.

S15- Consecutive-number maximum-value management file read-write competition prevention releasing

Completion

【図２】 **[FIG. 2]**



1-Computer which provides WWW service

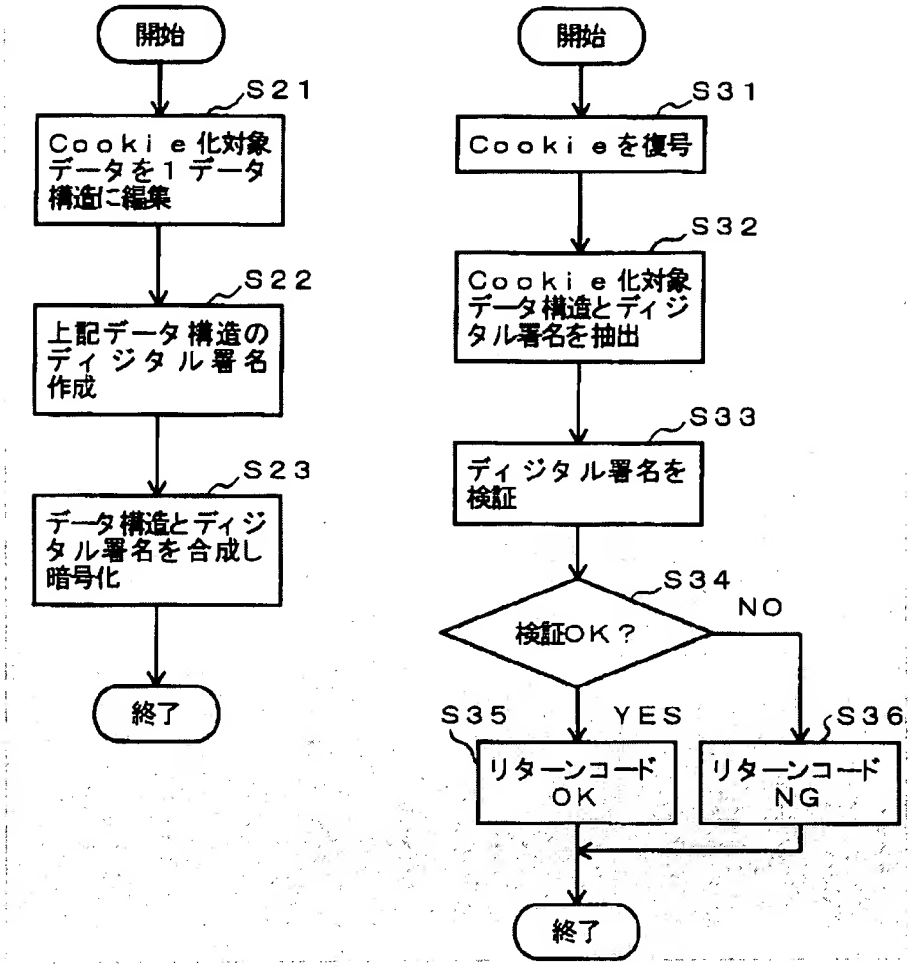
2- User terminal

-- start request for games-->
Consecutive number
The following area number
The total acquiring point
--> signature secret key
Digital signature
Encryption | Code following

game implementation <-- point game HTML
|
Acquiring point (20)

3-
Encryption | Encryption key
Series code
The following area number
Acquiring point (D)
<--> signature verification key
Digital signature
Encryption | Encryption key
game implementation <-- point game HTML

【図5】 **[FIG. 5]**



(A) Cookie generation part

Start

Data for formation of S21-Cookie are edited into 1 data structure.

Digital signature creation of the S22-above-mentioned data structure

S23-data structure and digital signature are compounded and it enciphers.

Completion

(B) Cookie verification part

Start

S31- Cookie is decoded.

S32- Data structure for Cookie-izing and digital signature are extracted.

S33- Digital signature is verified.

S34- Verification O.K.
S35- Return coding O.K.
S36- Return NG
Completion

THOMSON
DERWENT

DERWENT TERMS AND CONDITIONS

Derwent shall not in any circumstances be liable or responsible for the completeness or accuracy of any Derwent translation and will not be liable for any direct, indirect, consequential or economic loss or loss of profit resulting directly or indirectly from the use of any translation by any customer.

Derwent Information Ltd. is part of The Thomson Corporation

Please visit our home page: "WWW.DERWENT.CO.UK" (English)
"WWW.DERWENT.CO.JP" (Japanese)

